

**Congress of the United States**  
**Washington, DC 20515**

February 20, 2003

The Honorable Alan Greenspan  
Chairman  
Board of Governors of the Federal Reserve  
20<sup>th</sup> and Constitution Avenue, N.W.  
Washington, D.C. 20551

The Honorable John D. Hawke, Jr.  
Comptroller of the Currency  
Office of the Comptroller of the Currency  
Washington, D.C.

The Honorable James E. Gilleran  
Director  
Offices of Thrift Supervision  
1700 G Street, NW.  
Washington, D.C. 20552

The Honorable Timothy J. Muris  
Chairman  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

The Honorable Dennis Dollar  
Chairman  
National Credit Union Administration  
1775 Duke Street  
Alexandria, VA 22314

The Honorable William Donaldson  
Chairman  
Securities and Exchange Commission  
450 5<sup>th</sup> Street, NW.  
Washington, D.C. 20549

The Honorable Donald E. Powell  
Chairman  
Federal Deposit Insurance Corporation

February 20, 2003

Page 2

550 17<sup>th</sup> Street, N.W.  
Washington, D.C. 20429

The Honorable James E. Newsome  
Chairman  
Commodities Futures Trading Commission  
3 Lafayette Centre  
1155 21<sup>st</sup> Street, N.W.  
Washington, D.C. 20581

Dear Sirs:

I am writing in reference to your agencies' implementation of Section 501 ("Protection of Nonpublic Personal Information") of Title V of the Gramm-Leach-Bliley Act.

Recent press reports have indicated that computer hackers have obtained access to American Express, VISA, and Mastercard credit card information relating to approximately 8 million credit card accounts, breaking through the security protections of an un-named third party firm that processes credit card transaction information for merchants.

While I understand that this matter is the subject of an ongoing criminal investigation by the FBI, it also raises some important regulatory and compliance issues relating to the nature and adequacy of the security protections adopted by financial institutions to protect the security and privacy of consumers' nonpublic personal information. Allowing credit card information to get into the wrong hands could result in fraud, identity theft, and other illegal acts that could cause serious harm to consumers.

In response to concerns about this problem, Congress enacted Section 501 of the Gramm-Leach-Bliley Act. In Section 501, the Congress declared that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." In order to further this national policy, Congress directed each of your agencies to establish appropriate standards for the financial institutions subject to your jurisdiction relating to administrative, technical, and physical safeguards to:

1. "insure the security and confidentiality of customer records and information;
2. "protect against any anticipated threats or hazards to the security or integrity of such records;" and
3. "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer."

Each of your agencies has issued regulations to implement the requirements of Section 501. I would like to know whether, in light of aforementioned press reports, your

February 20, 2003

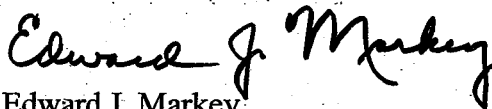
Page 3

agencies are concerned about whether the financial institutions you regulate are doing enough to safeguard the security and confidentiality of consumer credit card account information from computer hackers, either internally or when they contract with third parties. To the extent that any of the institutions you regulate may have been directly or indirectly affected by the recent hacker incident, have you conducted any investigations, examinations, or other inquiries to determine whether the institution's policies and procedures were in compliance with the rules your agency issued pursuant to Section 501? If so, what have you found? If not, why not?

If the financial institutions your agency regulates were not directly or indirectly affected by this recent hacker incident, have you conducted any examinations or inquiries to determine whether they might be vulnerable to similar hacker attacks? If so, have you found any similar vulnerabilities? If not, why not?

Thank you for your assistance and cooperation in providing responses to these questions. Should you have any questions about this inquiry, please have your staff contact Mr. Jeffrey S. Duncan of my office at 202-225-2836.

Sincerely,

A handwritten signature in cursive script that reads "Edward J. Markey".

Edward J. Markey  
Ranking Democrat  
Subcommittee on Telecommunications  
and the Internet